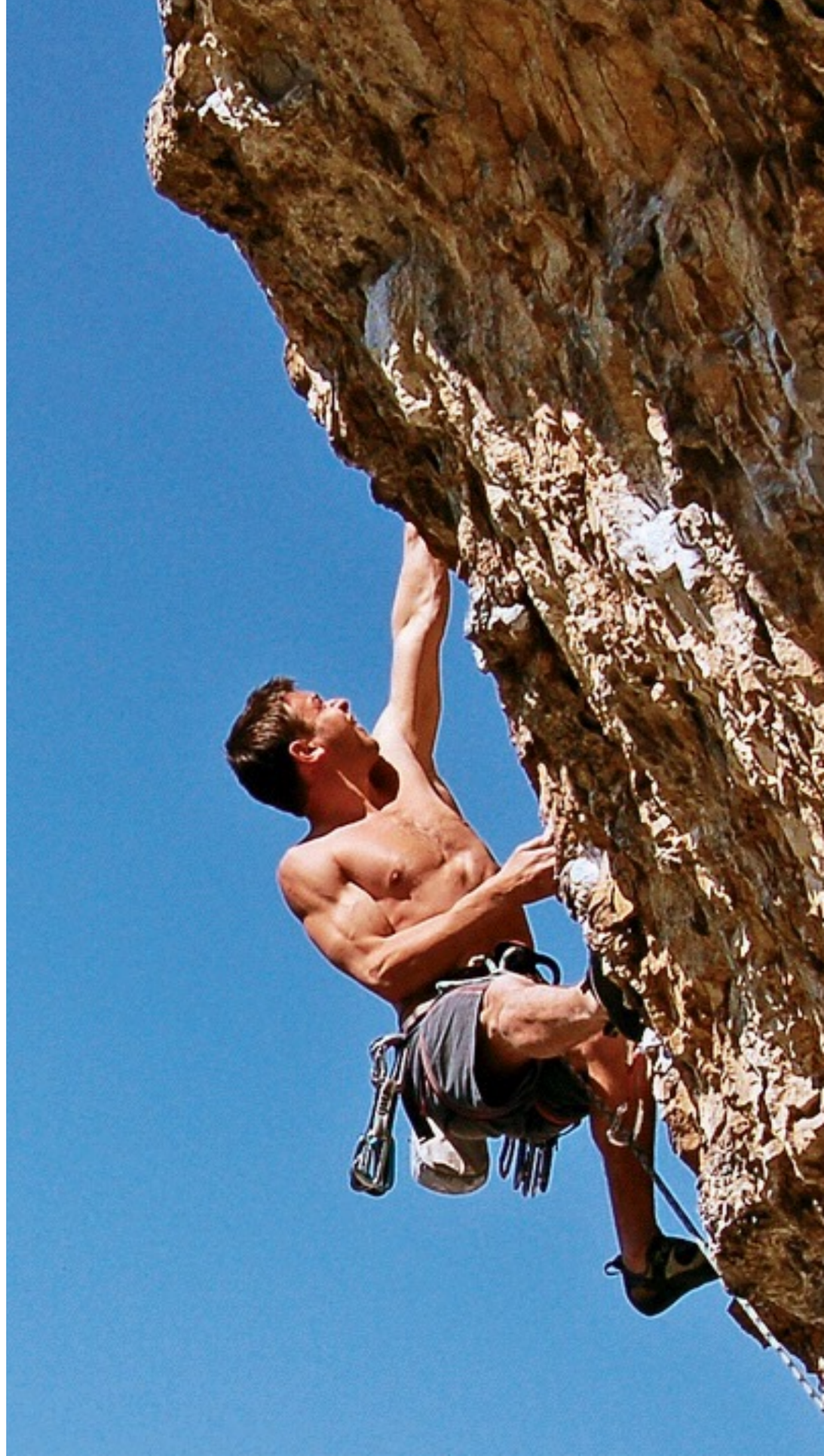
SECURITE ACTIF

version 7.1 @ fr_FR - Avril 2016

MISSION: IMPOSSIBLE

Un aperçu de la sécurité des sites web en 30’ (ou moins)

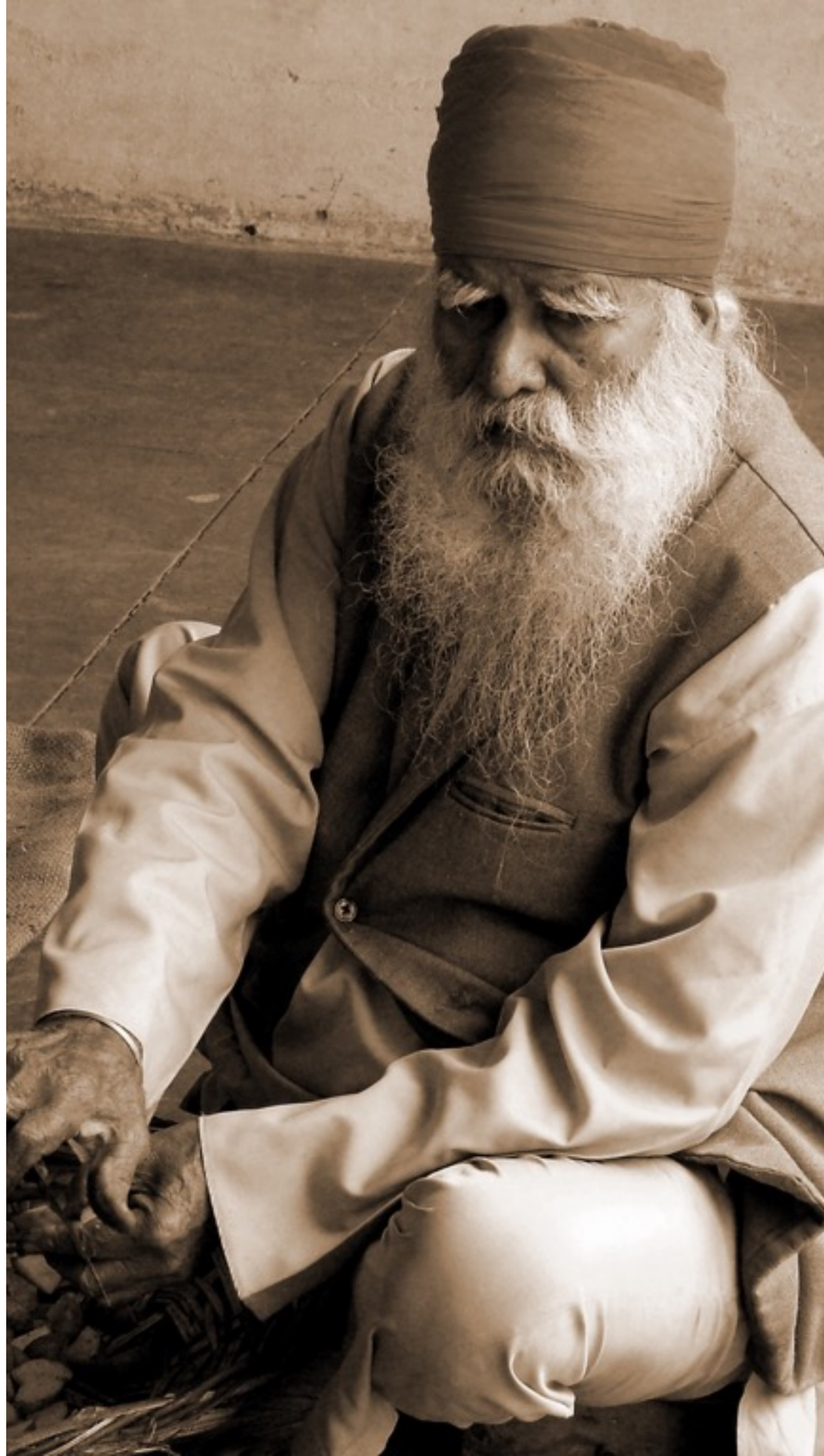


METTEZ VOS STYLOS DE CÔTÉ

Vous ne devez pas prendre des notes

J'AI DONNÉ CETTE PRÉSENTATION TROP LONGTEMPS...

Depuis 2010. C'est version 7.



DE NOUVELLES MENACES ONT ÉMERGÉ...

D'AUTRES SONT MAINTENANT EN DÉSUÉTUDE...

SURPRISE!

Les fondamentaux sont toujours les mêmes. Pour tout type de site.

METTEZ À JOUR VOTRE LOGICIEL DE SERVEUR

PHP, MySQL, Apache, SSH Server...

AUTORISATIONS & POSSESSION

Qui peut faire quoi et où

AUTORISATIONS & POSSESSION SAINS

- Tous les fichiers et les dossiers appartiennent à l'utilisateur du site (FTP / SFTP)
- Utilisez le mode FTP de Joomla! Sur les hébergeurs partagés horribles jusqu'à ce que vous convaincrez le client de déplacer le site à un hébergeur décent (ou de se débarrasser du çe client).
- **Dossiers**: autorisations **0755** • **Fichiers**: autorisations **0644**
- Si vous "devez" utiliser 0777 (vous ne le faites pas!), protégez vous avec un fichier .htaccess

```
order deny,allow
deny from all
allow from none
```

- Mieux encore, utilisez **FastCGI**

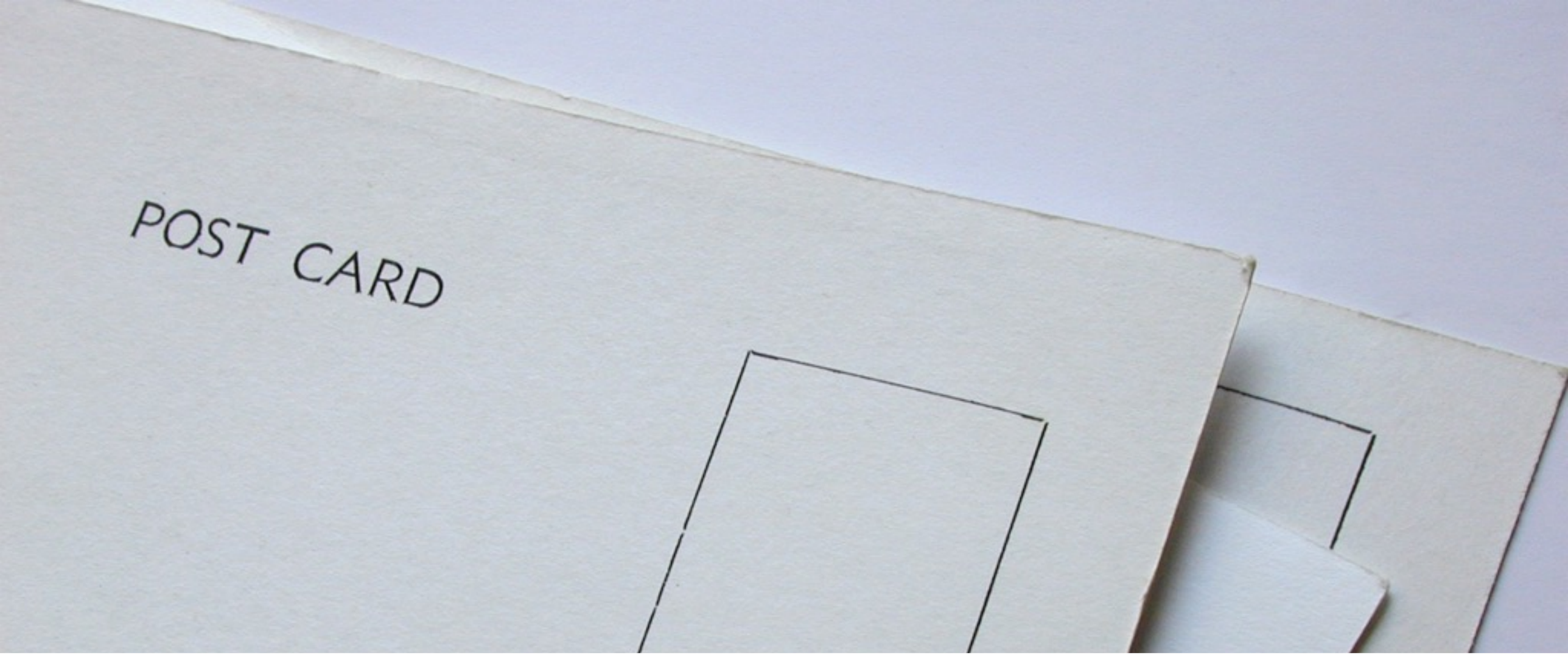
TROP DIFFICILE À MÉMORISER? RESSOURCES EN ANGLAIS.

- **Akeeba Backup User's Guide, Security Information**
  https://www.akeebabackup.com/documentation/akeeba-backup-documentation/security-info.html
- **777: The number of the beast**
  http://www.dionysopoulos.me/blog/777-the-number-of-the-beast

METTEZ À JOUR, HIER

Joomla! & extensions

PENSEZ AVANT D'INSTALLER



NE JAMAIS UTILISER FTP

Utiliser SFTP (transfert de fichiers via SSH)

LA LONGUEUR EST IMPORTANTE

LA LONGUEUR DE VOTRE MOT DE PASSE EST IMPORTANTE

MON DIEU, QUELLE MACHINE DE CRAQUAGE DE MOTS DE PASSE!

8 GPUs = 311.6 **milliards**
mots de passe **par seconde**

COMMENT

Mot de passe	Bits	Itérations	Temps de craquer
15082005	13,6	12416	0,04 picosec *(billionths of a sec)*
admin	15,9	61147	0,20 psec *(billionths of a sec)*
ortrtaortftaaidbt	67,7	2,39e+20	24.3 years
0rtrTA0rtfTa&idbT	88,2	3,55e+26	36 *million* years

Chiffré avec MD5 salée - Joomla! standard jusqu'à et incluant Joomla! 3.1

PENSEZ-VOUS QUE CELA EST EXAGÉRÉ?

La vitesse du craquage des mots de passe chiffrées avec MD5 a augmenté **d'un ordre de grandeur** au cours des quatre dernières années.

Password	Bits	Itérations	Temps de craquer
15082005	13,6	12416	0,04 µsec *(millionts of a sec)*
admin	15,9	61147	0,20 µsec *(millionts of a sec)*
ortrtaortftaaidbt	67,7	2,39e+20	24.3 *million* years
0rtrTA0rtfTa&idbT	88,2	3,55e+26	36 *billion* years

JOOMLA! 3.2+ UTILISE BCRYPT

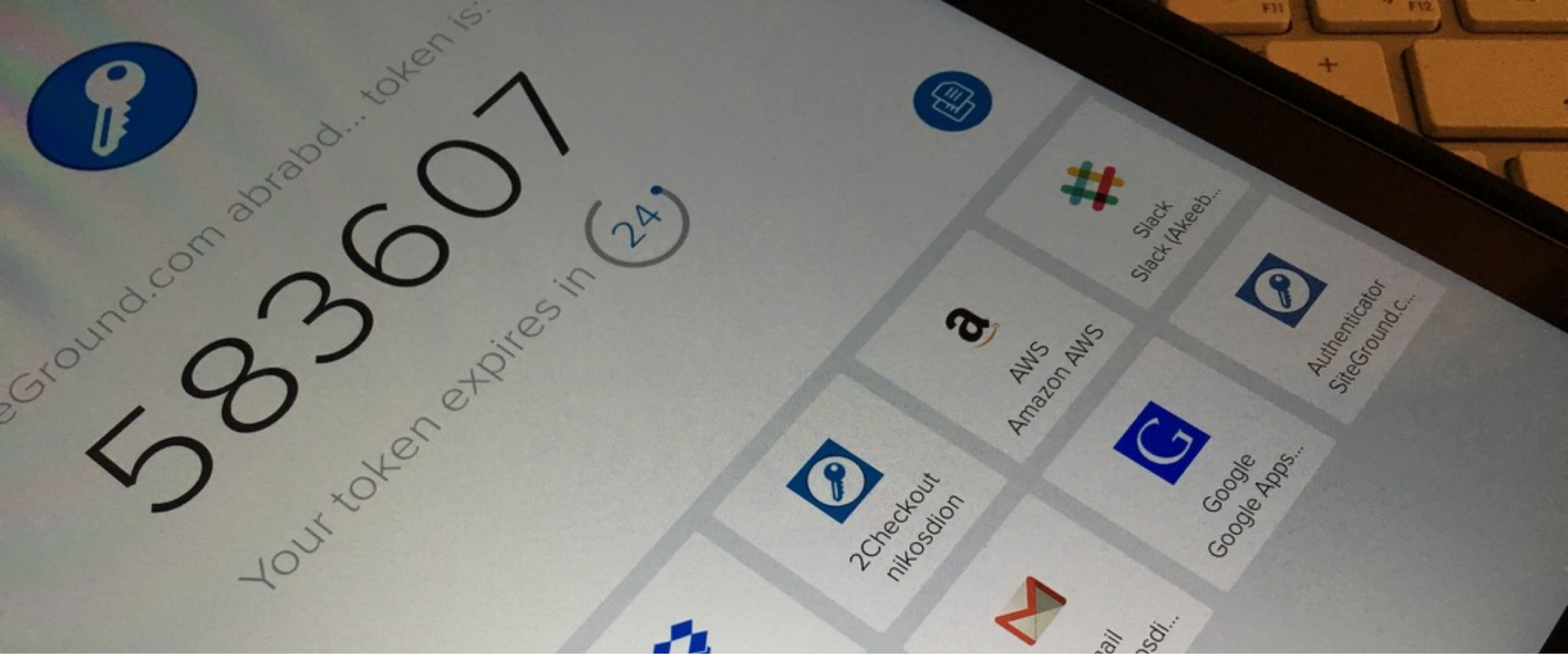
*Un million de fois **plus lent** de craquer que MD5*

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Et gardez-le sur votre personne (appareil mobile)

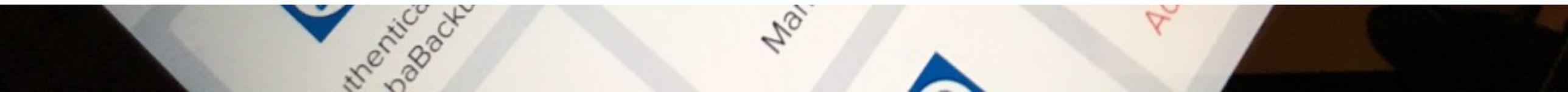
AUTHENTIFICATION À DEUX FACTEURS

*Quelque chose que vous **savez** et quelque chose que vous **avez***



CONSTRUIT DANS JOOMLA!

Authentification à deux facteurs avec Google Authenticator



CONSTRUIT DANS JOOMLA!

Authentification à deux facteurs avec YubiKey

NE PARTAGEZ PAS DES MOTS DE PASSE PAR EMAIL RÉGULIÈRE, NON CRYPTÉ

Ou sur les forums publics.

SUPPRIMEZ LES COMPTES TEMPORAIRES

Comme ceux que vous avez donné aux techniciens de soutien la semaine dernière…

SERRURE LE!

Rien sur mon site exécute à moins que je dis ça

RÈGLES .HTACCESS

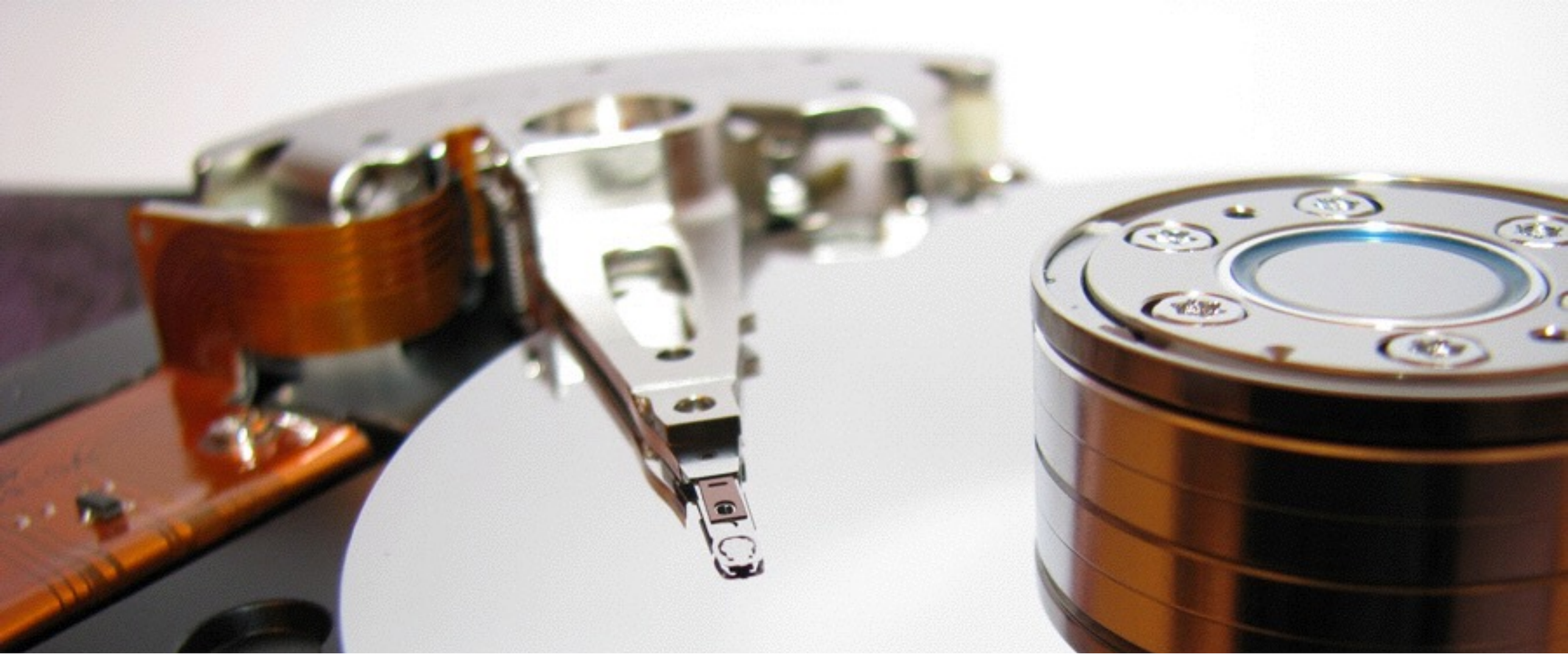
- **Mon Master .htaccess - GRATUIT**
  https://github.com/nikosdion/master-htaccess
- **Admin Tools Professional**
  https://www.akeebabackup.com/products/admin-tools.html

PROTÉGEZ VOTRE CONNEXION D'ADMINISTRATEUR

.htaccess (mieux) ou paramètre secret d'URL

METTEZ L'ARMURE

Protégez votre site



SAUVEGARDES

Fréquentes, automatiques, testés régulièrement, hors site

SURVEILLER LES CHANGEMENTS DE VOS FICHIERS

myJoomla.com, Admin Tools (PHP File Change Scanner)

PROTÉGER CONTRE DES ATTAQUES DDOS

par exemple utilisant CloudFlare CDN

EN DÉPIT DE TOUT ÇA....

MERDRE! VOUS ÊTES HACKÉ.

Maintenant, quoi?!

RESTEZ CALME

Ce n'est pas la fin du monde

NOUS AVONS DES INSTRUCTIONS (EN ANGLAIS)

- **De-hacker votre site**
  https://www.akeebabackup.com/documentation/walkthroughs/item/1124-unhacking-your-site.html
- Vous *avez* des sauvegardes, non?
- Vous *avez* utilisé myJoomla.com, non?
- Assurez-vous de lire les instructions avant d'être hacké.

ENCORE UNE CHOSE...

“

La sécurité n’est pas un projet.

La sécurité est un processus.

-Chaque expert en sécurité

QUESTIONS?

Voulez-vous les diapositives? http://akeeba.info/jd16fr

THANK YOU FOR LISTENING!

Voulez-vous les diapositives? http://akeeba.info/jd16fr